# PERIODIC SIGNALING SCHEME IN OBLIVIOUS DATA HIDING

*Litao Gang, Ali N. Akansu and Mahalingam Ramkumar*

New Jersey Center for Multimedia Research
Electrical and Computer Engineering Dept.
New Jersey Institute of Technology
University Heights, Newark, NJ 07102
{lxg8906,ali,mxr0096}@njit.edu

## ABSTRACT

*In the oblivious watermarking, information is extracted without reference to the original host signal, whose energy is much larger than that of the watermark signal. Suppressing host noise is a great concern. Some non-linear embedding methods, e.g. Quantization Index Modulation (QIM) can greatly suppress the host noise. In this method, the signaling is periodic. In this paper we analyze the Maximum Likelihood (ML) detector for the QIM signaling scheme, and compare the error probability with hard decision detector. Based on it, a new periodic signaling scheme is proposed and its optimum and suboptimal detection is derived. Through analysis and simulation, we demonstrate its advantage in term of PE-SNR over the existing methods.*

## 1. INTRODUCTION

Watermark or steganography is the technique to hide some information on a host signal (audio, video, image, etc.) without noticeable distortion. Watermark technique could be used for multimedia copyright protection and authentication.

Two basic requirements for watermarking are *robustness* and *transparency*. Transparency means the embedding should not degrade the image perceptual value. Robustness implies that the watermark should be robust against most common signal processing techniques, such as compression, filtering, or even some hostile attacks.

Watermark applications can be divided into two categories. One is *oblivious*, where detector does not require the original host. The other is *escrow*, where the detector need make reference to the original. In most applications, usually the original host is not available at decoder. In this paper, we focus on oblivious data hiding.

This work is partly supported by Panasonic Technologies, NJ

The greatest concern in oblivious application is host signal suppression. Some periodic signaling like Quantization Index Modulation (QIM) [1] is quite effective on this aspect. This nonlinear scheme is more successful than many linear embedding methods.

In Section 2, we describe the QIM scheme and analyze the Maximum Likelihood (ML) detection in Gaussian noise scenario. We also propose a suboptimal detector for implementation in practice. Simulation shows it outperforms some other detectors. In fact QIM embedding has long been used in some well-known schemes, such as parity manipulation. The main contribution of QIM is that soft decision detector can be used, thus greatly improves its performance.

In Section 3, a simple extension of QIM is proposed. The embedding and detection is discussed in detail. The same ML detection methodology can be applied. Simulation studies show that these methods outperform QIM at lower SNR.

In the last section, some conclusions are summarized.

## 2. QUANTIZATION INDEX MODULATION

### 2.1. QIM as a periodic signaling scheme

For the oblivious watermarking application, the greatest concern is host noise suppression. The original host signal is unknown and acts as noise. The Spread Spectrum modulation methods [4], [3] although successful in escrow case, is not quite effective in suppressing the host noise.

Chen and Wornell *et al.* [1], [2] applied dither modulation technique as a special case of quantization index modulation (QIM) for oblivious watermarking. It can achieve more reliable detection without referring to the original host signal.

Given a received coefficient $x$, a good estimate of the unknown original is its quantized version $Q(x, \delta)$

0-7803-6514-3/00/$10.00©2000 IEEE

where $\delta$ is the quantization step size. The embedded signal $s$ could be detected as

$$s = Q(x, \delta) - x. \tag{1}$$

The corresponding invertible embedding operator is

$$x = Q(c + s, \delta) - s, \tag{2}$$

where c is the original coefficient and $x$ is the marked coefficient after embedding.

Suppose an antipodal signal $s$ or $-s$ is to be embedded to hide information bit value 1 or 0. For example, if $c = 26.40$, $\delta = 1.0$, $s = 0.25$, the marked coefficient $x = Q(c + s, \delta) - s = Q(26.65, 1.0) - 0.25 = 26.75$. In a noise-free scenario, the detected signal $s' = Q(x, \delta) - x = 27.00 - 26.75 = 0.25$. In fact, to hide $s = 0.25$, the fraction of a marked coefficient $x$ should be 0.75 since $Q(\text{xxx.75}, 1.0) - \text{xxx.75} = 0.25$. Similarly, the fraction of $x$ embedded with bit value 0 should be 0.25.

The above embedding scheme can be interpreted as the following xoxo signaling. The original coefficient $c$ is replaced by the nearest point x to embed bit value 1 or to be replaced by the nearest point o to embed bit value 0. The embedding does not necessarily involve quantization operation.

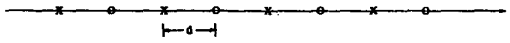


Figure 1: QIM periodic signaling

### 2.2. Maximum Likelihood Detection

In the Fig. 1, QIM is a periodic signaling scheme. Although the embedding operator (2) and extraction operator (1) are invertible in noise free scenario. It is far from optimum in noisy case.

Look at a specific example, suppose bit value 1 is embedded, the marked coefficient $x = 16.75$. After noise channel, if received value $r1 = 16.51$, the extracted signal $s' = Q(r1, \delta) - r1 = 0.49$. If $r2 = 16.49$ is received instead, $s' = Q(r2, \delta) - r2 = -0.49$! $r1$ and $r2$ are quite close, but result in two totally different extracted signals.

In detection, quantization operator may not be necessary. In this scheme, we need to decide a received coefficient $r$ comes from x points or from o points. The Maximum Likelihood (ML) ratio is [5]

$$R = \frac{P(x \in \text{set x}|r)}{P(x \in \text{set o}|r)}, \tag{3}$$

where $P(y|x)$ means given x, the probability of y. If $R > 1$, we decide the bit value is 1. Otherwise bit value 0 is decided.

The probability calculation is a little complicated. There exists many signal points corresponding to one information bit. On a received coefficient $r$, we know the transmitted signal $x$ could be xxx.75 or xxx.25. Suppose $r = 6.30$ is received, all the possible transmitted signals can be divided into 2 sets.

$$\begin{aligned} \textbf{Set1}: &\ \{\mathbf{6.75}, 5.75, 7.75, 8.75, 4.75, ...\} \\ \textbf{Set0}: &\ \{\mathbf{6.25}, 7.25, 5.25, 8.25, 4.25, ...\} \end{aligned}$$

Set 1 represents information bit value 1; Set 0 represents bit value 0.

If the noise is Gaussian distributed, its pdf is

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} exp(\frac{-x^2}{2\sigma^2}). \tag{4}$$

The probability $P(x \in \text{set } 1, r)$ can be calculated as

$$\begin{aligned} P(x \in \text{set } 1|r)P(r) &= P(r = 6.30|x = 6.75)P(x = 6.75) \\ &+P(r = 6.30|x = 7.75)P(x = 7.75) \\ &+P(r = 6.30|x = 5.75)P(x = 5.75) \\ &+... \end{aligned} \tag{5}$$

Similarly,

$$\begin{aligned} P(x \in \text{set } 0|r)P(r) &= P(r = 6.30|x = 6.25)P(x = 6.25) \\ &+P(r = 6.30|x = 5.25)P(x = 5.25) \\ &+P(r = 6.30|x = 7.25)P(x = 7.25) \\ &+... \end{aligned} \tag{6}$$

We assume the probabilities for all transmitting signals are equal, $P(x = 6.75) = p(x = 6.25) = p(x = 5.75) = ....$ Equation (3) can be reduced to

$$R = \frac{P(r = 6.30|x = 6.75) + P(r = 6.30|x = 5.75) + ...}{P(r = 6.30|x = 6.25) + P(r = 6.30|x = 7.25) + ...} \tag{7}$$

The above equation involves many terms, no closed-form result can be obtained. A suboptimal method needs to be used in practice. We define the dominating element in each set as *leader*. In our example, the leaders in Set 1 and Set 0 are $u = 6.75$ and $v = 6.25$. They are the most likely candidates. If all the remaining terms are neglected, the ML ratio (7) becomes

$$R \approx \frac{P(r|u)}{P(r|v)} = \frac{exp(\frac{-(r-u)^2}{2\sigma^2})}{exp(\frac{-(r-v)^2}{2\sigma^2})}. \tag{8}$$

This is the minimum distance detector. Our simulation shows the above is a good approximation for Gaussian noise environment.

### 2.3. Sequence Embedding and Detection

In most applications, a sequence s is embedded on c to enhance the reliability. Suppose one information bit

is embedded on 4 coefficients. We can define a deterministic pattern, for example, s = (x, o, x, o) where x and o stands for points in Set 1 and Set 0 respectively. Embedding is to modify $c_i$ so that it complies with the pattern s (to embed bit value 1) or with its reverse pattern $-\mathbf{s}$ = (o, x, o, x). At decoder, for every received coefficient $r_i$, find the leaders in Set 1 and Set 0, denote as $u_i$ and $v_i$. Therefore we can construct two most probable candidates

$$\mathbf{u} = (u_0, v_1, u_2, v_3), \tag{9}$$

and

$$\mathbf{v} = (v_0, u_1, v_2, u_3). \tag{10}$$

The approximation of ML detection is distance detector. If $||\mathbf{u} - \mathbf{r}|| < ||\mathbf{v} - \mathbf{r}||$, we decide the bit value is 1. Otherwise the decision is in favor of bit value 0.

For example, if $\mathbf{r} = (12.30, 7.12, 15.63, 16.34)$ is a received sequence, two leader candidates are,

$$\mathbf{u} = (12.75, 7.25, 15.75, 16.25)$$
$$\mathbf{v} = (12.25, 7.75, 15.25, 16.75)$$

Since $||\mathbf{x} - \mathbf{u}|| < ||\mathbf{x} - \mathbf{v}||$, the decision is bit value 1.

### 2.4. Performance Analysis

The idea of QIM has long been used in some watermarking algorithms. It is quite similar to the parity manipulation schemes. Some schemes in this category modify the parity of an integer coefficient $c$. For example, $c$ can be modified to an even number to embed bit value 1, or to an odd number to embed bit value 0. In [6], the DCT coefficients is modified in a similar way for image authentication. Its embedding procedure is, in essence, the same as QIM scheme. However, the detection used usually is hard decision detector, i.e. majority vote. In the above example, if even integers out-count odd ones, we decide bit value is 1. Otherwise it is decided 0. It is inferior to the above suboptimal detector which is a soft decision detector.

For comparison convenience, we redefine SNR as the ratio of watermark distortion energy to the noise power, i.e. $SNR = \frac{D}{\sigma^2}$. In real application, usually distortion energy $D$ is less than the noise energy, i.e. $SNR < 1$. Fig. 2 shows the simulation result for different detectors: the above suboptimal detector, quantization detector in (1), and majority vote detector.

The result shows the suboptimal method is the best. It demonstrates the same performance as the ML optimum detector.

The achievable error probability in QIM scheme is poorer than that achieved in the common binary antipodal communication model (Fig. 3). PE is calculated as the shadowed area in Fig. 4. The PE in QIM scheme at high SNR is $Q(\frac{d}{2\sigma})$ where $Q(.)$ is the Gaussian pdf tail integration function [1]. In practice, since data hiding usually works at low SNR, performance degrades significantly in periodic signaling compared with antipodal case. The gap between QIM and antipodal cases is depicted in Fig. 3.

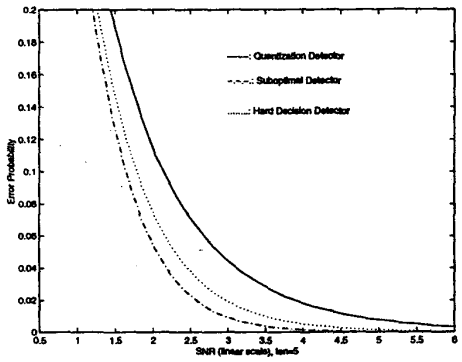



Figure 2: Detector Performance Comparison

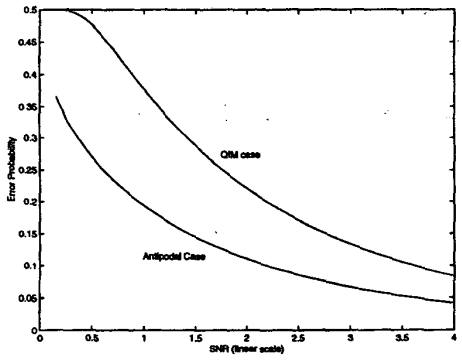
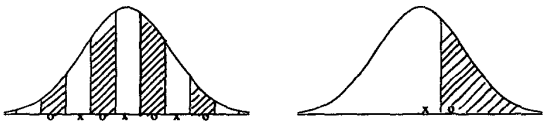



Figure 3: PE-SNR in QIM and Antipodal Case



(a) Periodic Signaling (b) Non-periodic Signaling

Figure 4: PE in Periodic and Non-periodic Signaling

## 3. AN EXTENSION OF PERIODIC SIGNALING SCHEME

In QIM scheme, suppose signal $x$ is transmitted, channel noise (positive or negative) tends to destroy it (deviates from x to o). As depicted in Fig. 4 (b), in the non-periodic signaling case, while negative noise is harmful,

the positive noise does not exert much harm on detection. Another heuristic periodic signaling is depicted in Fig. 5. It is clear that the noise in one direction is less harmful.

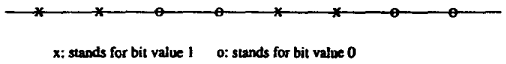



Figure 5: xxoo Periodic Signaling

The ML detection in this scheme can be derived in a way similar to that in Section 2. It is found ML optimum detection although theoretically computable, is too difficult to implement. Again a suboptimal method could be derived by considering only the nearest x and o points.

It is easy to see the distortion energy in this scheme is $D = \frac{7d^2}{12}$. More distortion is introduced than that in QIM scheme ($D = \frac{4d^2}{12}$). However, even taking it into consideration, simulation shows its PE-SNR performance is still superior to that in QIM.

In these two schemes, signaling is periodic and discrete. The Set 1 and Set 0 even need not to be discrete. We can further extend this idea to make Set 0 and Set 1 continuous instead of discrete (Fig. 6).

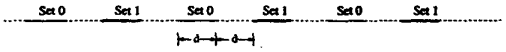



Figure 6: Continuous Set Periodic Signaling

The embedding is to keep the marked coefficient $x$ in Set 1 to embed bit value 1; or to keep it in Set 0 to embed bit value 0. The original coefficient $c$ is modified only if necessary.

Suppose the original coefficient $c$ is uniformly distributed and bit value 1 is to be embedded. After embedding, the error introduced is $e = x - c$. Consider a typical region AD (Fig. 7), if $c$ falls in the region AB, no modification is needed, $e = 0$. If $c$ is in the region BD. The error $e$ is uniformly distributed in the region of $(-3d/2, 3d/2)$. The conditional probabilities are $P(c \in AB | c \in AD) = 1/4$ and $P(c \in BD | c \in AD) = 3/4$. The average distortion introduced is

$$D = \frac{1}{4} \cdot 0 + \frac{3}{4} \cdot \frac{(3d)^2}{12} = \frac{9d^2}{16}. \qquad (11)$$

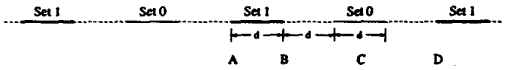



Figure 7: Distortion Calculation

The ML detection analysis can be applied at receiver. Further analysis shows since the possible transmitting signals are infinite, ML detector can not be reduced to a closed-form result. We can make an approximation by assuming the transmitted signals are from discrete points. If only the most probable candidates are considered, two useful suboptimal detectors are derived (Fig. 8).

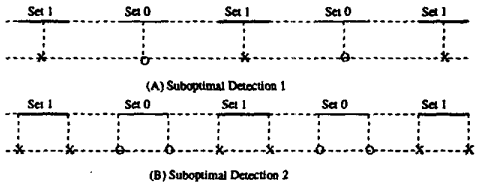



Figure 8: Suboptimal Detectors

Experiments demonstrate the suboptimal detector 2 is the better approximation than the method 1. Fig. 9 shows the performance of these two detectors in embedding 1 bit to a 11 coefficient sequence.

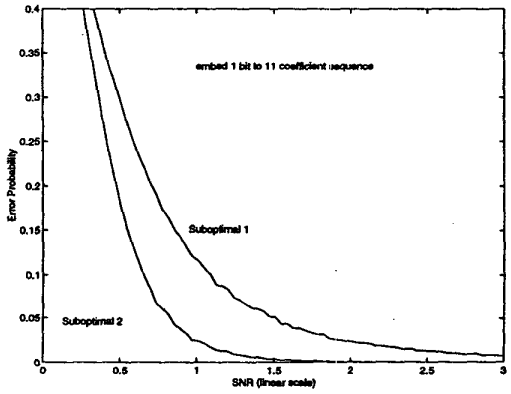



Figure 9: Suboptimal Detector Comparison

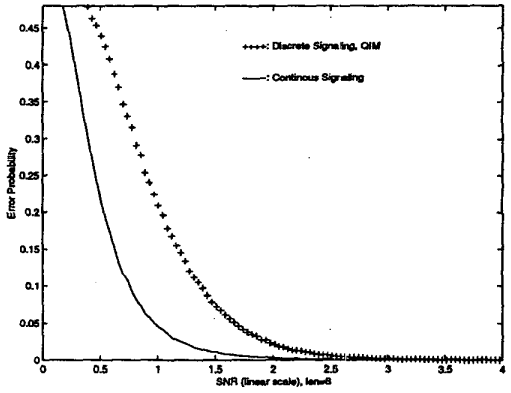



Figure 10: Performance Comparison at Lower SNR

We study the PE-SNR performance of the continuous signaling and QIM. Fig. 10 shows the result at

lower SNR. One information bit is embedded on an 8-coefficient sequence. The improvement of the continuous signaling over QIM is quite noticeable. That means at same distortion, the former is more reliable. Or it can achieve the same performance with less distortion.

At higher SNR, QIM scheme is slightly better than the continuous signaling scheme. Fig. 11 shows the result in embedding 1 bit on 4-coefficients. However, since watermarking always works at lower SNR, the continuous signaling is more promising. Especially it can achieve more reliable detection in a noisy scenario.

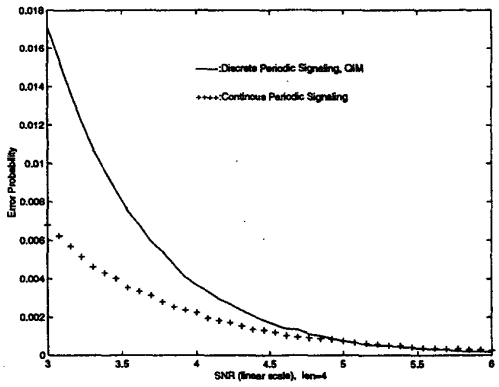



Figure 11: Performance Comparison at Higher SNR

## 4. CONCLUSIONS

1. In this paper, we discussed the QIM scheme and analyzed its ML optimum detector. For implementation purpose, we proposed a very good suboptimal detector. Simulation studies show its performance is almost the same as the optimum detector.

2. QIM is just a special case of the periodic signaling. Some other forms of periodic signaling, for example, continuous periodic signaling, can improve the performance. That is especially true at lower SNR, where practical watermarking applies. It is a promising algorithm and very robust in noisy scenarios.

3. The embedding of the periodic signaling is quite simple. The real challenge lies in detection. The optimum detector is computable in theory, but is not feasible in practice. Some suboptimal methods can provide satisfactory performance.

4. The periodic signaling should be kept private to enhance security. The original signaling can be shifted by a random value to make it more difficult to attack.

## 5. REFERENCES


[1] B.Chen and G.W. Wornell. "Dither Modulation: A new approach to digital watermarking and information embedding". *Proc. of SPIE: Security and Watermarking of Multimedia Contents*, 3657:344–353, Jan 1999.

[2] B. Chen and G. W. Wornell. "Digital watermarking and information embedding using dither modulation". *Proc. of 1998 IEEE Second Workshop on Multimedia Signal Processing (MMSP-98)*, pages 273–278, Dec 1998.

[3] I. Cox and M.L.Miller. "A review of watermarking and the importance of perceptual modeling". *Proceeding of Electronic Imaging*, Feburary 1997.

[4] I. J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. "A Secure, Robust Watermark for Multimedia". *Workshop on Information Hiding*, May 1996.

[5] Steven M. Kay. "Fundamentals of statistical signal processing". *Volume 2*, Prentice-Hall PTR, 1993.

[6] M. Wu and B. Liu. "Watermarking for Image Authentication". *Proceeding ICIP'98, Chicago, 1998*, 1998.